Cobb County...Expect the Best!

INTERNAL AUDIT DEPARTMENT
Report Number 2014-005

FINAL Letter Report – OnBase Security Investigation

November 3, 2014

Latona Thomas, CPA, Director
Steven Harper, Staff Auditor I
Barry Huff, Staff Auditor I

Table of Contents

November 3, 2014

MEMORANDUM

TO: David Hankerson, County Manager

FROM: Latona Thomas, CPA, Director

SUBJECT: **Final Letter Report** – OnBase Security Investigation

In August 2014, Information Services (I.S.) performed an analysis of accesses to the Department of Transportation (DOT) documents in a response to an inquiry from the Agency Director. In their analysis, they determined that one non-DOT employee had configured the OnBase[1] system to allow themselves full access to all DOT documents (approximately 780,000). I.S. also noted the employee had given themselves rights to access all documents in the Community Development (ComDev) repository (over 2.6 million). We were asked to investigate whether any of the DOT or ComDev documents in the OnBase repositories had been accessed and misused by the employee.

Executive Summary

We confirmed the employee configured their profile to allow access to the DOT documents. We did not have the records to confirm what actions were taken to gain access to the ComDev documents. Only two accounting related DOT documents and three ComDev documents have been accessed using the employee user name since April of 2007. The access to DOT documents appear related to a business need, and the ComDev director justified the employee's access to ComDev documents.

The employee had an improper security profile that allowed her to perform the configuration actions necessary to access the documents. The profile has been modified to provide the employee with rights to adequately maintain current departmental solutions. The employee must submit requests to the OnBase project team to conduct any other modifications to the department's current OnBase solution.

This report contains the results of additional security testing and steps taken by I.S. to strengthen the security controls so that all OnBase users have the proper security profile and their actions on the system are properly recorded for future review.

---

[1] The County's enterprise content management tool.

Recommendations

We recommended that I.S. give high priority to developing a security plan for the OnBase project. Other recommendations included acquiring and coordinating proper training, adherence to System Development Life Cycle principles, restoring the lost configuration log data and including in the future development of the enterprise-wide OnBase project, the non-DOT employee who has advanced OnBase knowledge and training.

Response

The Acting Information Services Director provided an initial response to our draft report. After discussion with the County Manager, I.S. was asked to modify their response to provide additional detail on the corrective action with proposed timelines. The new I.S. Director provided the modified response. She concurred with three of our five recommendations and proposed an acceptable alternative solution to the remaining two. The complete response to the draft report is included as Appendix III.

We thank employees in the Information Services, DOT, and Finance Departments for their cooperation in this review. We will perform a follow-up in six months on the implementation of the proposed corrective actions. In addition, Information Services will provide periodic updates on the corrective action directly to the County Manager. Copies of this report will be distributed to the managers affected by the report recommendations. Please contact me at (770) 528-2559 if you have questions or Barry Huff, Auditor-in-Charge at (770) 528-2558.

Results of Review

Inappropriate Access to Documents

We met with I.S. and identified the employee user name and the system location of the documents in question. We then independently validated the configuration log report, which provided a record of when and how the employee gained access to the DOT documents. We were unable to validate the same actions for the ComDev documents because the information was not available. Per I.S., the configuration data for some users was lost during an April 2014 system upgrade, and a request had been submitted to the software vendor to recover this data.

Using another systemic analytic tool, we reviewed the document history[2] for each of the documents in DOT and ComDev. This tool scans each document's history and lists what actions the document has been subject to including whether the document has been accessed, copied, modified or deleted.

Department of Transportation Documents

We determined that although the employee had access to all DOT documents, only two documents had been accessed. One accounts payable document was viewed and exported in August 2014; the other was viewed in December 2012. Based on the OnBase configuration and document history logs, there were no other actions taken on any other DOT documents using the employee's user name. I.S. informed us the employee had no other 'user name' on the system but did have access to another generic 'user name'. See '*Use of the 'Manager' and 'Admin' User Accounts*' section for additional discussion.

Community Development Documents

We also reviewed the document history report on ComDev documents and determined that the employee created or viewed three Business License documents in November 2013. The employee stated that there was a business need for accessing the documents as ComDev had requested assistance with the system development of their OnBase solution. I.S. confirmed this request with the Community Development Director. Our assurance regarding these documents is limited to the document history available.

Configuration Changes
After becoming aware of the I.S. analyses, configuration transaction logs showed the employee removed the changes made to the OnBase configuration that allowed access to both the DOT and ComDev documents. The employee acknowledged the negative appearance of such actions and acknowledged that, in hindsight, accessing the complete repository of DOT and ComDev documents was not necessary to respond to the requests for assistance.

---

[2] I.S. confirmed that the earliest entry date for the document history log is April 2, 2007.

Access to DOT Documents by Non-DOT Employees

We also requested and obtained a listing of 10 additional non-DOT employee users who recently[3] accessed the DOT documents. We reviewed the document histories for these users and determined that they had a business need to access the DOT documents. In addition, DOT management recently approved the continued access to the documents for nine of the 10 employees. One of the 10 employees did not have access rights to DOT documents but was emailed and then subsequently forwarded a DOT document to the employee in question. This employee made no direct accesses to DOT documents.

A synopsis of the accesses by these 10 employees is as follows: Information Services employees (3) provide support; Finance/Risk Management employees (2) need to process accounts payable documents and have access to lane closure permits; Water employees (4) need access to Utility Permits and one ComDev employee (two user names) is an ex-DOT employee who was granted extended permission by DOT to access their documents.

Security Profile Allowed Access to Documents

In our review, we evaluated the circumstances that allowed the employee access to documents outside of their department. Some of the documents have information and data that could be classified as 'Internal Use Only', 'Confidential' or 'Restricted Information' and should not be made readily available to anyone who does not have a business need.

We determined that the employee's system security profile allowed for substantial rights and permissions to configure the OnBase system. These rights, established in 2012 as a member of the initial OnBase project team, were too permissive for the user level, and were never monitored or modified. For example, the employee could set up user groups and establish security rights and permissions for themselves as well as for other users. Given this ability, the employee was able to establish themselves as a user in multiple groups carrying with them the inherited[4] rights received as an initial project team member. I.S. tried to limit the employee's access rights by modifying their rights in the main user group, but the employee was able to cancel the I.S. changes and reestablish the previous rights using their user identity established under a different group. The employee stated the rights and permissions were needed to balance and gather statistics on the department's workflow.

Corrective Actions Taken

The OnBase Project Manager has since modified the employee's rights and permissions to be in line with the business needs to oversee their department's solutions. This modification required the adjustment of rights to every occurrence of the employee's user account on the OnBase system. Moving forward, the employee is required to work with the OnBase Project team to make any further development changes or modifications to their solutions.

---

[3] Between July 22 and August 8, 2014.
[4] Unless restricted, when a user is assigned to another user group, they maintain the rights and permissions given when their initial user account was set up.

Additional Security Control Weakness

Use of the 'Manager' and 'Admin' User Accounts

According to I.S., the OnBase system comes configured with two user accounts: 'Manager' and 'Admin'. Any employee who knows the account password can utilize these accounts. Under these accounts, the user has high-level user rights that give them access to any document and permission to configure the OnBase system. Since the rights for these accounts are so encompassing, they should be assigned to one individual and used to perform actions other users cannot.

Our review showed the 'Manager' account password was known by at least six employees — four I.S. OnBase team members, one Finance department representative, and one Circuit Defender office representative. Any of the six could have used the account to access documents and reconfigure the system.

I.S. performed a document history analysis for the 'Manager' account and it showed the 'Manager' account accessed DOT documents between August 16, 2007 and September 8, 2014. Documents were exported, mailed, viewed, deleted, created and undeleted by an employee using the 'Manager' account. I.S. had no way to determine who was using the 'Manager' account during this period, although the project manager noted, after reviewing the report, that there were instances where team members could have used the account to provide support to DOT. **We cannot provide any assurance as to the work performed on the documents by the users of the 'Manager' account**.

Allowing multiple employee access to the 'Manager' account negates the benefit of the configuration and document history reports because anyone reviewing the reports can tell what actions were taken by the 'Manager' but the actual user is unknown. Those responsible for the system security cannot be assured the 'Manager' account is used appropriately.

According to a document history report, the 'Admin' account was used on seven dates, between May 1, 2007 to May 24, 2013, to view 17 documents and create two. I.S. informed us that the 2007 actions (three dates) were related to the initial set up and testing of the OnBase system. We were unable to validate the other fourteen accesses.

A National Institute of Standards and Technology article[5] stated:

"The most effective way to protect information and information systems is to integrate security into every step of the system development process, from the initiation of a project to develop a system to its disposition. The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system, is called the System Development Life Cycle (SDLC).

Security planning should begin in the initiation phase with the identification of key security roles to be carried out in the development of the system. The information to be processed, transmitted, or stored is evaluated for security requirements, and all stakeholders should have a common understanding of the security considerations. The Information System Security Officer (ISSO) should be identified as well.

---

[5] Shirley Radack, Editor, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistbul/april2009_system-development-life-cycle.pdf

Configuration management (CM) and control activities should be conducted to document any proposed or actual changes in the security plan of the system. Information systems are in a constant state of evolution with upgrades to hardware, software, firmware, and possible modifications in the surrounding environment. Documenting information system changes and assessing the potential impact of these changes on the security of a system are essential activities to assure continuous monitoring, and prevent lapses in the system security accreditation."

Corrective Actions Taken

I.S. informed us that they have reconfigured the OnBase system where project team members have the same rights as the 'Manager' account, but their individual activity on the system will be recorded under their respective user names. The password for the 'Manager' and 'Admin' accounts have been changed and secured between the OnBase Project Manager and Division Manager as backup. I.S. has also allocated funding from the Fiscal Year (FY) 2015 budget for the vendor to perform an overall security assessment of the OnBase security system including advice on the proper way to set up and use the 'Manager' and 'Admin' accounts.

In addition, I.S. has requested each department with OnBase to validate their current users. An assessment of each user's rights and permissions will be a part of the comprehensive security analysis that the vendor will provide. Written justification of business need and approval is now required for all added users to the OnBase system.

Recommendations

The Information Services Director should:

Recommendation 1: Make the development of **a security plan** for the OnBase project a priority issue to ensure that as the project is developed, security of the information stored on the system is properly protected from improper disclosure and accesses by individuals that do not have a need to review the information.

Auditee Response: *Information Services concurs with this recommendation.*

Planned Actions and Projected Completion
Funding was obtained in FY15 to address OnBase security in a phased approach within the ECM OnBase Program. The ECM Sponsors Group previously approved two priority Security projects for OnBase. The ECM Program Manager will now take back a recommendation to the sponsors to approve five priority Security projects. An Application Security Plan will be developed by Information Services which will include OnBase as the first application in the plan as noted below in Security Phase 3.

In addition, Information Services has reviewed and implemented revised configuration access rights in production. Configuration rights are now restricted to the ECM Team only which is in compliance with standard access protocols for all applications where Information Services is the system administrator.

The ECM Program Manager will continue to collaborate with Information Services Technical Operations and Client Services Divisions according to established security standards within the department per Information Services policy. Security, taxonomy, change control administration, and change management are included as priorities in the OnBase Expansion RFP (section 5 OnBase Service Deliverables) and EIA Report (section 2 Ready the Environment).

A four point approach to Program controls is available in EIA Report (section 5.3.2 Investing in Program Controls). This approach incorporates security among the standard controls for the Cobb ECM Program at the initiation of an OnBase project.

Actions included in each priority Security project are listed below:

- Security Phase 1 – Implement Periodic Self Audit of OnBase System

    o 1st audit completed on 8/15/2014

    o Provide quarterly updates to ECM Sponsors Group (user security updates/ changes)

    o Conduct OnBase Documents Audit by Department (semi-annually)

- Security Phase 2 – Implement Security Controls for OnBase Documents, Vendor/User Accounts and the Production Environment (Targeted completion 10/30/2014)

    o An OnBase Document Audit by Department was conducted for the 20 departments who currently use OnBase. (completed for 18 of 20 departments, 2 departments did not respond)

    o Vendor/User Account Security (completed)

    o Secure Production Environment (completed)

    See Appendix III for further details on Phase 2 of the security project.

- Security Phase 3 – Develop Information Services Application Security Plan to include the OnBase application (Target completion by 1/31/2015)

    o Develop 'Draft' Information Services Application Security Plan – by 12/31/2014

    o Approve 'Final' Information Services Application Security Plan – by 1/31/2015

    o OnBase will be the first application incorporated into the Information Services Application Security Plan

    o Integrate application system security best practices into System Development Life Cycle (SDLC) based on the National Institute of Standards and Technology (NIST) Security guidelines

    o Document, publish, and incorporate standards as they are defined

- Security Phase 4 – Conduct previously identified Vendor led Audit (as requested in RFP). Implement security guidelines for each OnBase project throughout 2015.

    o Interim security guidelines and SOPs were implemented and distributed to the ECM OnBase project team (until the Information Services Application Security Plan is completed)

    o Vendor led audit - *See Appendix III for further details on vendor led audit*

- Security Phase 5 – Establish SOPs and compliance requirements for: Security, Taxonomy, Change Management and Change Control Procedures. Security will be implemented on the security requirements of the specific project.
    - Interim security guidelines and SOPs were implemented and distributed to the ECM OnBase project team until the Information Services Application Security Plan is completed (completed 10/30/2014)
    - Final standards to be initiated during individual ECM Project implementations.
    - *See Appendix III for further details of Phase 5 of the security project.*

Recommendation 2: Ensure that the OnBase Project Team follows up with the software vendor to restore the missing portions of the configuration transaction log lost during the April 2014 system upgrade. Periodic status reports should be provided until the issue is resolved.

Auditee Response: Information Services concurs with this recommendation; however, the vendor has confirmed that we are unable to recover the missing configuration transaction logs.

Planned Actions and Projected Completion
Information Services escalated this matter through vendor support. The vendor advised that recovery is only possible if the logs are found on backup files. We conducted a search through database backups in an effort to recover the configuration transaction logs prior to April 2014. The prior logs were not found and cannot be restored.

Note: while the configuration transaction logs prior to April 2014 are not available, the actual OnBase configuration is intact within the OnBase database.

Actions taken and future plan to ensure no recurrence of this issue:

- Immediate removal of 'configuration transaction log purge' security rights to prevent future loss of configuration transaction logs (completed 8/13/2014)
- Investigate recovery of missing Configuration Transaction Logs – completed 10/30/2014
- Develop Configuration Transaction Log SOP – Targeted completion 11/30/2014

Better Coordination of OnBase Solution Development is Needed

Not all stakeholders in the development of the enterprise-wide OnBase document retention solution were collaborating to ensure that best project development practices were followed.

- Not all application solutions were created in the test environment prior to moving into the production environment.
- Change procedures were not being followed.
- Use of software licenses was not properly coordinated.

The employee in question developed several OnBase solutions to eliminate paper and create more efficient systemic workflows. These solutions were developed without much collaboration with the OnBase project team.

The employee obtained additional training, coordinated with the local OnBase vendor, and took the initiative to develop these solutions. At the time of initial development, an OnBase project team had not been identified and there were no centralized enterprise-wide collaboration efforts. The delay in establishing a centralized function and lack of synergy with the project team allowed development without conforming to established best practices and system development controls.

According to I.S. and review of transaction logs, it appears that most of the design and development of the solutions were done in the 'production' mode of the OnBase system rather than in the 'test' environment. I.S. has established a test environment for the development of OnBase solutions that mirrors the production environment. The test environment should be used to perform testing of proposed OnBase solutions and changes to established solutions. I.S. also established a change protocol that requires all changes to established solutions be tested and analyzed by the project team to ensure its compatibility with OnBase and other network applications. According to I.S., changes were made in the production environment without adhering to the change protocol.

The Document Import Processor software is used to import large volume of documents into the system. The license for the software must reside on the server or workstation using the software. Coordinating the DIP license use was not performed to ensure the enterprise-wide operation of the OnBase application. The employee in question assigned the license from the enterprise server to their workstation without coordination with the project team; this could have affected the operation of the enterprise-wide OnBase application. Although the employee contends that the license can be reassigned without much effort, for the benefit of the enterprise-wide application, the assigning of software license should be under the control of the project team. Reassigning the license without knowledge of how it affects the operation of other enterprise-wide applications is negligent.

We believe including the employee in the enterprise-wide implementation of OnBase is essential to take advantage of the additional training and working knowledge of OnBase and working within the framework of the project development best practices and controls is essential for the successful enterprise-wide implementation of OnBase.

Recommendations

The Information Services Director should:

Recommendation 3: Discuss the inclusion of the employee with their expertise, advanced training and working knowledge on the enterprise-wide implementation of the OnBase solution. They should be utilized to help the County achieve its enterprise-wide goals and projects. A specific time commitment to the project should also be negotiated.

Auditee Response: Information Services concurs with this recommendation.

Planned Actions and Projected Completion
In addition, multi-departmental project core teams will be included in OnBase projects to leverage institutional business knowledge, advanced training, technical experience and expertise from employees across the county. Subject Matter Experts (SMEs) and Business Process Owners are essential to a successful enterprise ECM solution. Inclusion of these resources will be utilized to help the County achieve its enterprise-wide and department specific goals and projects.

9

Appropriate time commitments to each OnBase project is required as a critical success factor from the Core Team members.

See Appendix III for the complete response to Recommendation 3.

Recommendation 4: Ensure training for all members of the OnBase project team are commensurate with the system development needs. The training and knowledge of the team members should be coordinated with project development goals.

Auditee Response: Information Services concurs with this recommendation and proposes additional training guidelines.

Planned Actions and Projected Completion
Information Services concurs with the recommendation regarding training for all members of the OnBase project team.

In addition, to ensure Program continuity, adequate support, appropriate infrastructure build out and configuration; Information Services proposes that all OnBase training be coordinated through the ECM Program Manager, or their designee, which is similar to the training program found within the county's GIS program. Training will be scheduled to compliment skills requirements for the projects and priorities as set by the ECM Sponsors group. This will ensure just in time training for all Cobb resources.

Information Services included training at all levels of the organization in the OnBase Enhancement RFP and EIA Report. A summary of the training component of the ECM Program is available in the EIA Report (section 5.3.1 Investing in the Internal Team).

See Appendix III for the complete response to Recommendation 4.

Recommendation 5: Ensure the OnBase Project team follows established SDLC principles in providing oversight and guidance to the development of all OnBase projects. A thorough knowledge of the security requirements of the system should be obtained and integrated in all future system development.

Auditee Response: IS Concurs with this recommendation and proposes SDLC principles be followed by all participants on OnBase projects.

Planned Actions and Projected Completion
Established SDLC principles are included in the OnBase Enhancement RFP (section 5 Service Deliverables & 6 Professional services) and in the EIA Report (section 3.6 Shared Solution Attributes and 3.7 Common Project Tasks). The OnBase Enhancements RFP specifically required PMBOK or similar SDLC methodology which outlines clearly defined phases. Each project in the ECM Program will utilize either the waterfall, agile, or hybrid approach. These are all examples of SDLC.

In addition, Information Services recommends adherence to SDLC guidelines as a requirement for all OnBase Administrators, OnBase Liaisons, Project Core Team Members, Business Process Owners, SMEs, End Users, etc. Everyone involved in an OnBase Project must adhere to these standards to ensure a successful and timely implementation.

Additionally, compliance with change management and change control standards is essential to ensure the OnBase Project Team is fully briefed on all changes introduced into the Enterprise ECM system. The project manager will take the lead in assigning and tracking task completions on projects, and is empowered to escalate to management as needed to mitigate risks. The ECM Program Manager is authorized to implement SOPs and oversee cross-training as needed to ensure compliance with the methodology.

- Establish SDLC SOPs (include required artifacts, design reviews, change management, change control, etc.) (11/30/2014)

- Cross-train OnBase Administrators and project participants in SDLC (included with each project)

- Monitor compliance with SDLC methodology (i.e. signed acknowledgements, review artifacts, provide feedback/guidance, etc)

Abbreviations and Glossary

OnBase	In addition to document imaging, OnBase is a collection of technologies (100 plus tools) used to capture, store, access, process, integrate and measure business information across an organization.
ComDev	Community Development
DOT	Department of Transportation
I.S.	Information Services
SDLC	System Development Life Cycle is a conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application.

Final Report Distribution List

Willie Hopkins, Support Services Agency Director
Sharon Stanley, Information Services Director
Ed Biggs, Acting Information Services Director
Julia Levesque, Information Services Division Manager
Yolanda Rucker, OnBase Project Manager
Jim Pehrson, CPA, Comptroller/Finance Director
Faye DiMassimo, Transportation Agency Director
Rob Hosack, AICP, Community Development Agency Director
Deborah Dance, County Attorney
Internal Audit Department File

Auditee Response

INFORMATION SERVICES

100 Cherokee Street, Suite 520
Marietta, Georgia 30090-7000
Phone: (770) 528-8700 Fax: (770) 528-8706

Sharon A. Stanley
Director

DATE: October 31, 2014

TO: Latona Thomas, CPA, Director, Internal Audit

FROM: Sharon Stanley, Information Services Director

SUBJECT: Response to the Internal Audit Division's Letter Report – OnBase Security Investigation

This memo is in response to the subject report dated October 8, 2014. In the analysis found in the report, you determined that although an employee had inappropriately accessed another department's OnBase document repository, only two documents had been accessed, and those documents were related to a request for assistance from that department. Also, though all other documents were fully available to the employee, no other documents were determined to have been accessed and used in an inappropriate manner. Your analysis also determined that the security protocols and privileges within the OnBase system were such that misuse of the documents, whether or not on purpose, was a risk. You made several recommendations to help ensure the security and integrity of the OnBase system and to provide for a successful and repeatable project management approach for the further development of the OnBase system. Our responses to those recommendations are found below.

The Information Services Director should:

Recommendation 1: Make the development of **a security plan** for the OnBase project a priority issue to ensure that as the project is developed, security of the information stored on the system is properly protected from improper disclosure and accesses by individuals that do not have a need to review the information.

Response: *Information Services concurs with this recommendation:*

Planned Actions and Projected Completion

Information Services concurs with this recommendation. Funding was obtained in FY15 to address OnBase security in a phased approach within the ECM OnBase Program. The ECM Sponsors Group previously approved two priority Security projects for OnBase. The ECM Program Manager will now take back a recommendation to the sponsors to approve five priority Security projects. An Application Security Plan will be developed by Information Services which will include OnBase as the first application in the plan as noted below in Security Phase 3.

In addition, Information Services has reviewed and implemented revised configuration access rights in production. Configuration rights are now restricted to the ECM Team only which is in compliance with standard access protocols for all applications where Information Services is the system administrator.

The ECM Program Manager will continue to collaborate with Information Services Technical Operations and Client Services Divisions according to established security standards within the department per Information Services policy. Security, taxonomy, change control administration, and change management are included as priorities in the OnBase Expansion RFP (section 5 OnBase Service Deliverables) and EIA Report (section 2 Ready the Environment).

A four point approach to Program controls is available in EIA Report (section 5.3.2 Investing in Program Controls). This approach incorporates security among the standard controls for the Cobb ECM Program at the initiation of an OnBase project.

Actions included in each priority Security project are listed below:

14

- Security Phase 1 - Implement Periodic Self Audit of OnBase System
    - 1st audit completed on 8/15/2014
    - Provide quarterly updates to ECM Sponsors Group (user security updates/changes)
    - Conduct OnBase Documents Audit by Departments(semi-annually)

- Security Phase 2 – Implement Security Controls for OnBase Documents, Vendor/User Accounts and the Production Environment (Targeted completion 10/30/2014)
    - An OnBase Document Audit by Department was conducted for the 20 departments who currently use OnBase. (completed for 18 of 20 departments, 2 departments did not respond)
        - Distributed three Audit Reports to department heads
            1. Report 1 - Identify who has access to department documents
            2. Report 2 – Summary Report to remove anyone who should not have access to department documents
            3. Report 3 - Identify who has viewed department documents within 1 month
    - Vendor/User Account Security (completed)
        - Develop User account request forms (to add, modify, deactivate OnBase Users)
        - Develop Vendor account request form (eliminate generic accounts, create unique vendor user accounts with access to TEST environments)
    - Secure Production Environment (completed)
        - Restrict configuration access in production database (limit access to OnBase Change Control Administrators)
        - Secure passwords for administrative accounts (Manager, Administrator); restricted to ECM Program Manager and OnBase Change Control Administrator
        - Restrict rights to view transaction logs (OnBase Core Team only)
        - Eliminate security access to purge transaction logs (remove security rights)
        - Sensitive Documents SOP – remove access to county sensitive documents (such as HR, Medical Examiner, Juvenile Court, etc)
        - Retire Obsolete User Groups SOP – delete user security groups no longer in use and groups with excessive privileges

- Security Phase 3 – Develop Information Services Application Security Plan to include the OnBase application (Target completion by 1/31/2015)
    - Develop 'Draft' Information Services Application Security Plan – by 12/31/2014
    - Approve 'Final' Information Services Application Security Plan – by 1/31/2015
    - OnBase will be the first application incorporated into the Information Services Application Security Plan
    - Integrate application system security best practices into System Development Life Cycle (SDLC) based on the National Institute of Standards and Technology (NIST) Security guidelines
    - Document, publish, and incorporate standards as they are defined

- Security Phase 4 – Conduct previously identified Vendor led Audit (as requested in RFP). Implement security guidelines for each OnBase project throughout 2015
    - Interim security guidelines and SOPs were implemented and distributed to the ECM Onbase project team (until the Information Services Application Security Plan is completed)
    - Vendor led audit will include
        - Analysis of current user security model and recommend best practice standard for an enterprise OnBase implementation
        - Specific emphasis on Active Directory/OnBase user group synch, user group privileges, network authentication options
        - Recommendations for support team model (roles/responsibilities) for enterprise implementation

2

- Recommendations of best practice approach for security migrations across environments (TEST, QA, Production)
  - Security Phase 5 – Establish SOPs and compliance requirements for: Security, Taxonomy, Change Management and Change Control Procedures. Security will be implemented on the security requirements of the specific project.
    - Interim security guidelines and SOPs were implemented and distributed to the ECM Onbase project team until the Information Services Application Security Plan is completed (completed 10/30/2014)
    - Final standards to be initiated during individual ECM Project implementations.
    - Examples:
      - Separate privileges across user security groups (i.e. view, print, create, modify, delete, configure, etc)
      - Change Control (migrating changes across environments – advanced notification & documentation requirements)
      - Configuration Management (who is authorized to configure various application features/functions such as: users, user groups/rights, keywords, scripts, disk groups, etc)
      - Remove default naming convention for web servers, application servers, application pools (establish secure, unique naming convention)
      - File security (manage file shares using advanced utilities – to restrict ability to navigate to files using unc paths)

Recommendation 2: Ensure that the OnBase Project Team follows up with the software vendor to restore the missing portions of the configuration transaction log lost during the April 2014 system upgrade. Periodic status reports should be provided until the issue is resolved.

Response: *Information Services Concurs with this recommendation; however the vendor has confirmed that we are unable to recover the missing configuration transaction logs.*

Planned Actions and Projected Completion

Information Services escalated this matter through vendor support. The vendor advised that recovery is only possible if the logs are found on backup files. We conducted a search through database backups in an effort to recover the configuration transaction logs prior to April 2014. The prior logs were not found and cannot be restored.

Note: while the configuration transaction logs prior to April 2014 are not available, the actual OnBase configuration is intact within the OnBase database.

Actions taken and future plan to ensure no recurrence of this issue:

- Immediate removal of 'configuration transaction log purge' security rights to prevent future loss of configuration transaction logs (completed 8/13/2014)
- Investigate recovery of missing Configuration Transaction Logs -- completed 10/30/2014
- Develop Configuration Transaction Log SOP – Targeted completion 11/30/14

Recommendation 3: Discuss the inclusion of the employee with their expertise, advanced training and working knowledge on the enterprise-wide implementation of the OnBase solution. They should be utilized to help the County achieve its enterprise-wide goals and projects. A specific time commitment to the project should also be negotiated.

Response: *Information Services Concurs with this recommendation*

Planned Actions and Projected Completion

Information Services concurs with this recommendation. In addition, multi-departmental project core teams will be included in OnBase projects to leverage institutional business knowledge, advanced training, technical

3

experience and expertise from employees across the county. Subject Matter Experts (SMEs) and Business Process Owners are essential to a successful enterprise ECM solution. Inclusion of all these resources will be utilized to help the County achieve its enterprise-wide and department specific goals and projects.

Appropriate time commitments to each OnBase project is required as a critical success factor from the Core Team members. Listed below are examples of active projects with multi-departmental resources. The Core Team has been notified for each project and requested to identify potential schedule conflicts for the next quarter. Detailed project plans and project calendars are being finalized at this time.

- o ePlan for Site Plan Review Project – multiple departments (Target completion Spring 2015)
- o Circuit Defender Case Management Project– 2 departments (Target completion Spring 2015)
- o Finance/Advanced Capture Project- 6 pilot departments (Target completion Spring 2015)

Recommendation 4: Ensure training for all members of the OnBase project team are commensurate with the system development needs. The training and knowledge of the team members should be coordinated with project development goals.

Response: *Information Services Concurs with this recommendation and proposes additional training guidelines*

Planned Actions and Projected Completion
Information Services concurs with the recommendation regarding training for all members of the OnBase project team.

In addition, to ensure Program continuity, adequate support, appropriate infrastructure build out and configuration; Information Services proposes that all OnBase training be coordinated through the ECM Program Manager, or their designee, which is similar to the training program found within the county's GIS program. Training will be scheduled to compliment skills requirements for the projects and priorities as set by the ECM Sponsors group. This will ensure just in time training for all Cobb resources.

Information Services included training at all levels of the organization in the OnBase Enhancement RFP and EIA Report. A summary of the training component of the ECM Program is available in the EIA Report (section 5.3.1 Investing in the Internal Team).

- o Training for OnBase project team (ongoing)
- o Training at all levels within the County (ongoing)
- o Registration for OnBase Training coordinated through Information Services

Recommendation 5: Ensure the OnBase Project team follows established SDLC principles in providing oversight and guidance to the development of all OnBase projects. A thorough knowledge of the security requirements of the system should be obtained and integrated in all future system development.

Response: *Information Services Concurs with this recommendation and proposes SDLC principles be followed by all participants on OnBase projects*

Planned Actions and Projected Completion
Information Services concurs with this recommendation. Established SDLC principles are included in the OnBase Enhancement RFP (section 5 Service Deliverables & 6 Professional services) and in the EIA Report (section 3.6 Shared Solution Attributes and 3.7 Common Project Tasks). The OnBase Enhancements RFP specifically required PMBOK or similar SDLC methodology which outlines clearly defined phases. Each project in the ECM Program will utilize either the waterfall, agile, or hybrid approach. These are all examples of SDLC.

In addition, Information Services recommends adherence to SDLC guidelines as a requirement for all OnBase Administrators, OnBase Liaisons, Project Core Team Members, Business Process Owners, SMEs, End Users,

4

etc. Everyone involved in an OnBase Project must adhere to these standards to ensure a successful and timely implementation. Additionally, compliance with change management and change control standards is essential to ensure the OnBase Project Team is fully briefed on all changes introduced into the Enterprise ECM system. The project manager will take the lead in assigning and tracking task completions on projects, and is empowered to escalate to management as needed to mitigate risks. The ECM Program Manager is authorized to implement SOPs and oversee cross-training as needed to ensure compliance with the methodology.

- o Establish SDLC SOPs (include required artifacts, design reviews, change management, change control, etc.) (11/30/2014)
- o Cross-train OnBase Administrators and project participants in SDLC (included with each project)
- o Monitor compliance with SDLC methodology (i.e. signed acknowledgments, review artifacts, provide feedback/guidance, etc)

Recommendation 1: Security Plan
Reference: OnBase Expansion RFP (section 5 OnBase Service Deliverables)

---

5 *"OnBase" Services – Service Deliverables*

As part of the professional services requested in this RFP, the Cobb County Information Services request the selected vendor to do the following:

5.01 *Documentation*
The selected vendor shall create and provide the following documentation in the course of the project:
1) Documentation of recommended and/or performed Configuration changes so that Cobb may gain expertise in-house of the application
2) A Communications Plan
3) A Formal Project Implementation Guide (Project Plan)
4) Curriculum of recommended End User Classes along with training materials
5) Training plan for the implementation of new modules
6) Training plan for administration training
7) Recommendations for structuring OnBase support team
8) Recommendations for change control management

5.02 *Infrastructure*
Create a finalized infrastructure analysis with recommendations regarding:
1) Necessary changes for anticipated growth
2) Load balancing as needed
3) Number of environments needed to support business processes and implementation of additional modules

5.03 *Configuration Set Up*
1) Conduct an audit and analysis of current configuration and recommend best practices
2) Implement best practice configurations

Recommendation 1: Security Report
Reference: EIA REPORT (section 2 Ready the Environment)

Ready the OnBase Environment / Team Before work on system configuration can begin, Cobb/Harvest will need to prepare the technical environment and begin the process to expand the OnBase team at Cobb. Development of the OnBase team is critical to ensure Cobb is capable of maximizing OnBase investments. *Hyland Note₁:* This activity aligns with strategic goals to provide sound technology infrastructure and maintain highly skilled resources. Investment in the OnBase team will allow Cobb to expand OnBase more rapidly.	2.1 PROGRAM - Secure 2014 licensing 2.2 PROGRAM - Secure professional services 2.3 PROGRAM - Build the OnBase team 2.4 PROGRAM - Set 2014 OnBase training plan 2.5 ONBASE - Build DEV, TEST, PROD environments 2.6 ONBASE-Upgd hardware to v13 specifications Env 2.7 ONBASE - Upgrade to v13 2.7 ONBASE - Deployment for OnBase v13 2.8 ONBASE – DDS, HSI PW, KOMpliance (Security) **2.8 ONBASE – System Audit & Security (Phase 1)** **2.8 ONBASE – System Audit & Security (Phase 2)** 2.9 ONBASE - Standardize on the OnBase Unity Client 2.10 PROGRAM - Create a Taxonomy committee 2.10 PROGRAM - Scanner Replacements (Phase 1) 2.10 Evaluate/Update Taxonomy Standards/Guidelines 2.11 PROGRAM - Define Change Management Controls 2.12 PROGRAM - Define Common Project Controls 2.13 PROGRAM - Checkpoint to evaluate Staff Aug. needs

Recommendation 1: Security Plan

Attachments

Reference: EIA REPORT (section 5.3.2 Investing in Program Controls)

5.3.2 Investing in Program Controls

In addition to people, successful (OnBase) programs endorse the processes and procedures (controls) to ensure solutions are on-point. It is common for organizations to overlook the importance of such controls, though they are necessary to maintain a healthy and sustainable (OnBase) program. Having the proper controls in place will allow Cobb to thoughtfully introduce and support new OnBase solutions in production settings.

Recommended Actions:

Using the table below, the easiest way to introduce controls in a developing (OnBase) program is to model it after programs applied to other critical systems used by Cobb, such as existing LOB's. Assuming these controls meet Cobb requirements, Cobb can reuse such policies for the management and support of OnBase. The key here is to have the strategy in place and make sure a process is place to guide each of the activities listed in the table below. Introduction of the controls below will help to protect the integrity of planned solutions.

Hyland Note: All program controls are not required day 1, but should be addressed over the life cycle of the 2014 Roadmap. Start this activity as part of **Step 2: Ready the Environment**

Example (OnBase) Program Controls:

IS / Business	ECM / OnBase
1 Standard IS Controls • Business Continuity and/or DR Planning • Capacity Planning • Security Planning • Technology Road Map • Technical Training • Work Order Process	**3 Standard ECM Controls** • Classification/Taxonomy (see next section) • Information Inventory • Records Retention (Management) Policy
2 Standard Business Controls • Access and Security • Enterprise Road Map • User Testing Plan • User Training Plan	**4 Important OnBase Controls** • Change Management Policy • Incremental Release Strategy • Migration Strategy (DEV->TEST->PROD) • Team Training • Upgrade Strategy

Hyland Note: Regarding Security -- (1) If departmental resources report to IS, they may be granted security rights in production, based on change control procedures. (2) If departmental resources report to the department, they will be granted security rights in TEST, based on change control procedures as defined by Cobb.

Recommendation 2: Restore Missing Transaction Logs
No reference for this section

Recommendation 3: Include Employees Expertise / Knowledge
Reference: EIA REPORT (section 3.7 Common Tasks Key Participants/Actions)

3.7 Common Project Tasks (OnBase Solutions)

The following table contains a listing of project tasks to be applied during steps 3, 4 and 5 of the Roadmap. Though duration per activity will change based on the solution being delivered, Cobb divisions can expect the following methodology (approach) to be followed by the teams implementing OnBase.

Common Project Tasks:

Task	Key Participants /Actions	Outputs / Dependencies[1]
1 Discovery This task will require Cobb IS and Harvest Services teams to meet with impacted business users to define low-level solution requirements. Solution requirements will be used to define the full scope of the project, validate budgetary estimates and complete/update the detailed project plan	• Cobb SMEs, IS, Harvest • Lead: Cobb IS & Harvest • Key Contributors: Cobb SMEs • Document the current process, requirements • Agree to solution scope, inclusions • Finalize budget, professional services estimates	• Solution Requirements Document (SRD) • A minimum of (2) SMEs per department • Management and user participation is key • Business users should expect 5-10 days of participation per solution
2 Design/Build This task will require Cobb IS and Harvest Services teams design and build the OnBase solution using low-level solution requirements.	• Cobb SMEs, IS, Harvest • Lead: Cobb IS & Harvest • Design and build the OnBase Solution • Solutions are configured in OnBase DEV • Execute functional testing • Present progress (weekly) to collect feedback	• (Signed) Solution Requirements Document[2] • OnBase Solution delivered for UAT • Business users should expect 3-5 days of participation to validate requirements, review progress and confirm the SRD is satisfied
3 User Acceptance Testing (UAT) This task will require Cobb IS and SMEs to design and execute testing cases to ensure the OnBase solution meets business requirements and is ready for a production release to end users	• Cobb SMEs, IS, Harvest • Lead: Cobb IS & SMEs (Harvest to support) • Solutions are migrated to OnBase TEST • Design and execute test cases (SMEs) • Design and execute performance test cases • Cobb IS / Harvest to manage/remedy issue logs	• (Closed) Solution Requirements Document • Delivered OnBase Solution • Business users should full participation (5-10 days) • UAT is a minimum of 10 days *Hyland Note:* This step in the methodology is driven primarily by Cobb. Harvest's role in this step will be primarily to resolve any issues that surface during testing.

Attachments

Recommendation 3: Include Employees Expertise / Knowledge
Reference: EIA REPORT (section 3.7 Common Tasks Key Participants/Actions)

Task	Key Participants /Actions	Outputs / Dependencies[1]
4 Training, Release This task will require Cobb IS, Cobb SMEs and Harvest to migrate/release the OnBase solution to production. This task will also require Cobb to communicate updates to the business and retrain users as needed. It is highly recommended that training take place by department and includes SMEs to support the transition to new configurations.	• Cobb SMEs, IS, Harvest • Lead: Cobb SMEs, Cobb IS & Harvest • Design and execute communication plans • Design and execute end user training • Provide 'extra' training to designated SMEs • Design and execute solution release • Solutions are migrated to PROD (OnBase Team) • Execute post-release support (approx. 10 days) • Revisit trained areas within 30 days to answer questions, retrain as necessary and evaluate solution health in the adopting business area	• (Approved) User Acceptance Testing • Business users should expect 5-10 days of participation to train end users and provide support to the release of the solution *Hyland Note:* Training end users is a critical task for the OnBase team when new solutions are implemented. This task will require Cobb to define training procedures when releasing new capabilities to the business.

[1] The actual number of days for each task will vary by project. Cobb IS and Harvest will estimate the duration/effort during project planning steps.

[2] It will be very important for Cobb/Harvest to manage initial project scope. Best demonstrated practice is to give users time to use the solution for a period of time as non-essential requirements tend to change after use.

Recommendation 4: Training
Reference: OnBase Expansion RFP (sections 5.04 Training OnBase Team)

5.04   Training (Details in Section 6.03)

1) Provide Certification Training for Cobb County OnBase support team. :

   Certification Training can be performed or recommended in any combination of the following ways:
   - a) A "public" certification class hosted at Cobb and attended by both County employees and people outside of the County which defrays some of the cost
   - b) Performed by Hyland at another facility as part of their regular certification training
   - c) Performed by Hyland at Cobb facility specifically for only Cobb
   - d) Via training.OnBase.com – As specified by Vendor.
   - e) Via Hyland Premium Subscription – As specified by Vendor. (Cobb already has a subscription)
   - f) If certified, the selected vendor may lead the certification classes at a Cobb facility.

   Proposer shall provide cost for option recommended in proposal.

2) Recommend, Develop and Provide curriculum and initial classes for End User training utilizing the train-the-trainer approach. Vendor would initially teach the end-user classes and provide materials to us to continue training.

3) Develop training materials to be used by the various classes.

Reference: Recommendation 4: Training
Reference: OnBase Expansion RFP (sections 6.03 Training County Staff)

6.03   County Staff Training

The proposer shall prepare a training plan for County staff that will enable them to operate and support the system. Developing a full training curriculum and executing training is part of the deliverables of this project. For evaluation and cost purposes, the proposer will give a draft training plan for the planning and teaching the following:

   - a. Certified Administrators (OCSA) – 5 people
   - b. Additional Certified Training as Recommended by Vendor – 4 people
   - c. End User Training within Selected Departments (Identified in Section 5.06: Train-the-Trainer Approach for their specific modules/solutions) – 5-10 People in each department
   - d. End User Training for End Users outside of Selected Departments for features/functionalities as recommended by Vendor in curriculum (20 hrs – Specific curriculum to be determined) – 75-100 people

The proposed plan shall be refined as a final deliverable upon project initiation.

It shall include any courses to be provided off-site, classroom training, and on-the-job training necessary for OnBase Certified and End User training. End User training shall be conducted at Cobb County's facilities that support 12-15 students per class.

The training plan provided shall include estimates for time spent in each type of training and what method will be used to execute the training. It shall also indicate how the required certification training shall be performed. See section 5.04 for list of options.

Attachments

Recommendation 4: Training
Reference: EIA Report (sections 5.3.1 Training Internal Team)

5.3 Keys to a Sustainable OnBase Program (People, Process, Technology)

Investment in people, process and technology will be critical to encourage document management and workflow growth, execute the included roadmap and enable long-term success (stability). This section quickly introduces the commitments and activities commonly adopted by peer organizations seeing successes in the delivery of OnBase and related workflow campaigns.

5.3.1 Investing in the Internal Team

Cobb will need to build an internal (OnBase) team to fully benefit from available solutions and ultimately, lower the total cost of ownership. This team should consist of members on the (Core) IS team to support the program as a whole, and also include individuals within each department/division at Cobb as necessary to be a main point of contact when performing discovery, implementing, or testing solutions.

Leadership Roles and Expected Responsibilities:

Leadership	Administrative	Build	Supporting
1 Executive Sponsor • Sponsors the OnBase program • Set strategy, goals and vision • Communicates value to users • Inspires departmental commitments • Set budgets and secure investments *Internal Source: IS / Business Area*	**1 (OnBase) Sys Admin** *(Cobb: Lead OnBase Admin.. OnBase Admin.)* • Manage the general configuration of OnBase • Manage the general performance of OnBase • Provide high level administration, maintenance and support • Owns (OnBase) solutions locally *Training: OnBase certified technical administrator* *Internal Source: IS / Business Area*	**1 Project Manager** *(Cobb: Project Manager)* • Project lead and team coordination • Manage scope, resources, time and project budgets • Administer project controls, status, and change/issue mgmt. *Internal Source: IS / Business Area*	**1 Business SME (OnBase Liaison)** • Business process and req. definition • Testing, training and release support • Full process ownership for the dept • Scan/index as necessary
2 Business Sponsor • Sponsors the OnBase program locally • Defines business goals • Inspires user commitments • Drives business transformation *Internal Source: Business Area*	**2 (OnBase) Work Mgt. Admin** *(Cobb: Workflow Engineer)* • Manage workflow configurations in OnBase • Provide high level administration, maintenance and support • Owns (OnBase) workflow solutions locally *Training: OnBase certified workflow (case mgr.) administrator* *Internal Source: IS / Business Area*	**2 Functional Analyst** *(Cobb: Business Analyst)* • Supports discovery and recording of business requirements • Brokers communications between business and IS • Leads solution testing, training and release activities • (optional) Supports solution discovery, configuration *Internal Source: IS / Business Area*	**2 Records Analyst** • Bus. record definition (taxonomy) • Administer Records retention policy **3 Application Analyst** *(Cobb: Integrations Specialist)* • Manage/support bus. applications • Drive conversations between teams *Internal Source: IS / Business Area*
3 Program Lead • Set (OnBase) strategy, goals and vision • Set (OnBase) technical architecture • Oversees the OnBase team • Oversees OnBase controls • Oversees OnBase taxonomy *Internal Source: IS*	**3 (OnBase) Imaging & Index Team** *(Cobb: Doc. Imaging Specialist)* • Manage capture configurations in OnBase • Execute capture process flows (scanning) in OnBase • Classify (index) content imported into OnBase *Training: Internal training by Sys or Workflow Admins* *Internal Source: IS / Business Area*	**3 Solution Engineers** *(Cobb: Workflow Administrator)* • Provide solution discovery and design • Provide base configurations (e.g., doc types, keys, security) • Configure system capture, import and delivery methods • Configure work management system (e.g., Workflow) • Provide functional, regression and migration testing *Internal Source: IS / Business Area*	**4 Database Analyst** • Database server setup & administration • Database backup policy ownership **5 Network/Infrastructure Analyst** • Network design and architecture • OnBase server setup & administration • OnBase envt. (Dev, Test, Prod) support
Hyland Note[1]: Invest in this role early. Most OnBase projects are impacted negatively without visible support/backing of internal sponsors that are well-liked across the business. *Hyland Note[2]: Influence is a key differentiator. Resources (especially sponsors) will ensure that business decisions are made quickly. This trait is also very helpful to encourage business transformation (change) that is often common with the introduction of new technologies.*	*Hyland Note[1]: Harvest and/or Hyland may provide professional services here until Cobb procures the internal team.* *Hyland Note[2]: Experience is valuable, but not necessary. If experience is not an option*	*Hyland Note[1]: Harvest and/or Hyland may provide professional services here until Cobb procures the internal team.* *Hyland Note[2]: Business and technical skills are both required. The very best OnBase team resources possess a "hybrid" of business and technical skills. Business skills help to ensure that the right OnBase solution is designed, while technical skills ensure that*	**6 Security/Compliance Analyst** • Set corporate compliance strategy • Set legal, policy & procedure reqmts • Set security roles, rights and restrictions *Internal Source: IS / Business Area* **7 Reporting Analyst** *(Cobb: Reporting Analyst)* • Report design and architecture • Reporting setup & administration • Services to administer reports **8 Security/Compliance Analyst** • Set corporate compliance strategy • Set legal, policy & procedure reqmts. • Set security roles, rights and restrictions *Internal Source: IS / Business Area* **9 Harvest and/or Hyland Services** • Services to design & build solutions

Attachments

Recommendation 5: SDLC
Reference: OnBase Expansion RFP (section 5 OnBase Service Deliverables)

---

5   *"OnBase" Services – Service Deliverables*

As part of the professional services requested in this RFP, the Cobb County Information Services request the selected vendor to do the following:

5.01   *Documentation*
The selected vendor shall create and provide the following documentation in the course of the project:
1) Documentation of recommended and/or performed Configuration changes so that Cobb may gain expertise in-house of the application
2) A Communications Plan
3) A Formal Project Implementation Guide (Project Plan)
4) Curriculum of recommended End User Classes along with training materials
5) Training plan for the implementation of new modules
6) Training plan for administration training
7) Recommendations for structuring OnBase support team
8) Recommendations for change control management

5.02   *Infrastructure*
Create a finalized infrastructure analysis with recommendations regarding:
1) Necessary changes for anticipated growth
2) Load balancing as needed
3) Number of environments needed to support business processes and implementation of additional modules

5.03   *Configuration/Set Up*
1) Conduct an audit and analysis of current configuration and recommend best practices
2) Implement best practice configurations

5.07   *Support Recommendations*

We expect the Vendor to recommend industry best practices for internally supporting the OnBase solution across the County. This would include recommendations on how to best manage change control either through workflow and/or configuration migration. We want the Vendor to revisit these recommendations at the end of the engagement that considers our unique business constraints and deliver final recommendations in a written report.

5.09   *Best Practices Recommendations*

The selected vendor would make Best Practices Recommendations from an enterprise support perspective for the following during the course of the project:
1) Evaluate number of licenses necessary for each module based on anticipated business use.
2) Evaluate current configuration setup and make recommendations that best suit the business needs of Cobb.
3) Review security setup to ensure it effectively meets the needs of an enterprise solution for the County.
4) Evaluate additional functionality for use in various business processes. Additional functionality may be implemented along with module implementations to achieve goals as explained in Section 5.06. Or it might be recommendations as a method to achieve future goals.

Attachments

Recommendation 5: SDLC
Reference: OnBase Expansion RFP (section 6 Professional Services)

---

6   Professional Services

Cobb County wishes to find a vendor that has application expertise; we require the following documents to be included in the proposer's response.

6.01   Project Definition

The proposal should include an executive summary describing an overall implementation plan. This proposed plan shall be refined as a final deliverable upon project initiation.

A sample of previous Implementation Plans shall be included. Either by the sample or by list, the proposer shall indicate why types of artifacts are normally produced in their Final Implementation Plan.

The proposer must include hours to evaluate the current system/business processes and procedures and recommend necessary changes to effectively and most efficiently expand OnBase functionality. These services shall be extensive with the proposer providing most of the effort in both documenting/integrating business processes and configuration of the system. However, there should be enough training during the implementation to allow the County to change and support the system as needed after implementation is complete.

6.02   Project Management

Cobb County uses the Project Management Institute's (PMI) Project Management Body of Knowledge Guide (PMBOK) methodology as a project management best practice.

The proposer should describe their experience in implementing and managing projects using PMBOK or a similar project management methodology. The proposer should also include what tools or techniques they will use to effectively manage this project.

The county is particularly interested in how the proposer's project management approach utilizes the following or similar key process groups when implementing a project. Also, the proposer should provide documentation which shows their understanding of the application of such documents within each key process group.

1) **Initiating** - Setting up the project for success by identifying the right team (especially the project manager) and scope, as well as determining the relationship between the project and its alignment with the client's overall objectives.

2) **Planning** – Developing the relevant resources, timelines and milestones, and aligning project deliverables to business priorities (i.e. risk management, communications, quality, cost/budgeting, duration and sequencing, external dependencies).

3) **Executing** – Assigning a project team and distributing information to ensure the proper project activities are undertaken. This process also includes ensuring quality assurance methods are in place to address change management.

4) **Controlling and Monitoring** – Ensuring the resulting project activities is in check with the original project charter and plan, and risk from uncontrolled external actions is mitigated.

   a. Monitor quality, costs and schedule;

   b. Manage stakeholder relationships, risk and contract monitoring;

   c. Identify discrepancies (or variations) within the project schedule to ensure project schedule is met.

   d. Ensure proper project communications

5) **Closing** – Making sure you have delivered everything expected of the project.

Attachments

Recommendation 5: SDLC
Reference: EIA Report (section 3.6, 3.7 Shared Solutions & SDLC Methodology)

3.6 Shared Solution Attributes

The following table contains a listing of solution tasks and/or features expected to provide value across individual OnBase Solutions. Separated out to reduce replication in the tables above (sections 3.3, 3.4 and 3.5). Cobb/Harvest teams are expected to apply the techniques below during the delivery of new or updated OnBase solutions at Cobb (e.g. CONTRACTS -- Files & Folders, HR -- Capture, Access, Files & Folders).

Shared Solution Tasks:

Task	Key Participants /Actions	Outputs / Dependencies
1 Taxonomy This task will require Cobb to review and assess current OnBase document type and keyword configurations to identify challenges, opportunities to reuse classifications across cross-functional processes and business requirements for planned updates. Ultimately, this task will help Cobb identify challenges (duplicates) in current designs and visible relationships between information assets that can be used to enhance OnBase capture solutions and the design of OnBase folders, custom queries and cross-references *Additional Information:* Refer to **appendix section 5.3.3** for more information	• Cobb SMEs, IS, Harvest • Export current classifications from OnBase • Consolidate duplicates • Define/map document relationships • Define/map security requirements • Consolidate keyword instances • Identify KTG opportunities • Define folder configurations • Define common searches (custom queries) • Define 'personal page' views (by user role) • Evaluate versioning requirements in OnBase	• Manage the taxonomy inventory in MS Excel • Review and update the taxonomy for every new OnBase solution • Business users should be heavily involved • Cobb IS will 'own' the taxonomy at a centralized point *Hyland Note[1]* Hyland/Harvest may provide a database script to extract current configurations for Cobb to leverage as a start point to the taxonomy exercises *Hyland Note[2]* The conversion of prior documents/keywords may be executed through direct database updates and/or use of workflow to re-index documents as necessary
2 Capture Solutions This task will require Cobb to update and/or create new methods for users to more easily capture documents into the OnBase solution. For example, this task includes steps to install the Outlook integration which will allow users to import and index emails and attachments directly from their native email client *Additional Information:* Refer to **section 4.3.1** for more information.	• Cobb IS, Harvest • (Optional) Pilot the solution in State Court • Review, update capture steps • Evaluate barcodes to ease indexing • Evaluate AE, autofill to ease indexing • Evaluate interactive data capture • Add the OnBase Outlook Client • Add other Office integrations • Add drag-and-drop to folders • Evaluate adding Hyland print driver	• OnBase 13 installed • Taxonomy effort is started • New licensing installed • Pilot in State Court is completed • **Solution discovery** is completed (by department) • (Optional) OnBase Unity Client is installed

3.7 Common Project Tasks (OnBase Solutions)

The following table contains a listing of project tasks to be applied during steps 3, 4 and 5 of the Roadmap. Though duration per activity will change based on the solution being delivered, Cobb divisions can expect the following methodology (approach) to be followed by the teams implementing OnBase.

Common Project Tasks:

Task	Key Participants /Actions	Outputs / Dependencies[1]
1 Discovery This task will require Cobb IS and Harvest Services teams to meet with impacted business users to define low-level solution requirements. Solution requirements will be used to define the full scope of the project, validate budgetary estimates and complete/update the detailed project plan.	• Cobb SMEs, IS, Harvest • Lead: Cobb IS & Harvest • Key Contributors: Cobb SMEs • Document the current process, requirements • Agree to solution scope, inclusions • Finalize budget, professional services estimates	• Solution Requirements Document (SRD) • A minimum of (2) SMEs per department • Management and user participation is key • Business users should expect 5-10 days of participation per solution
2 Design/Build This task will require Cobb IS and Harvest Services teams design and build the OnBase solution using low-level solution requirements.	• Cobb SMEs, IS, Harvest • Lead: Cobb IS & Harvest • Design and build the OnBase Solution • Solutions are configured in OnBase DEV • Execute functional testing • Present progress (weekly) to collect feedback	• (Signed) Solution Requirements Document[2] • OnBase Solution delivered for UAT • Business users should expect 3-5 days of participation to validate requirements, review progress and confirm the SRD is satisfied
3 User Acceptance Testing (UAT) This task will require Cobb IS and SMEs to design and execute testing cases to ensure the OnBase solution meets business requirements and is ready for a production release to end users.	• Cobb SMEs, IS, Harvest • Lead: Cobb IS & SMEs (Harvest to support) • Solutions are migrated to OnBase TEST • Design and execute test cases (SMEs) • Design and execute performance test cases • Cobb IS / Harvest to manage/remedy issue logs	• (Closed) Solution Requirements Document • Delivered OnBase Solution • Business users should expect full participation (5-10 days) • UAT is a minimum of 10 days *Hyland Note:* This step in the methodology is driven primarily by Cobb. Harvest's role in this step will be primarily to resolve any issues that surface during testing.

Task	Key Participants /Actions	Outputs / Dependencies[1]
4 Training, Release This task will require Cobb IS, Cobb SMEs and Harvest to migrate/release the OnBase solution to production. This task will also require Cobb to communicate updates to the business and retrain users as needed. It is highly recommended that training take place by department and includes SMEs to support the transition to new configurations.	• Cobb SMEs, IS, Harvest • Lead: Cobb SMEs, Cobb IS & Harvest • Design and execute communication plans • Design and execute end user training • Provide 'extra' training to designated SMEs • Design and execute solution release • Solutions are migrated to PROD (OnBase Team) • Execute post-release support (approx. 10 days) • Revisit trained areas within 30 days to answer questions, retrain as necessary and evaluate solution health in the adopting business area	• (Approved) User Acceptance Testing • Business users should expect 5-10 days of participation to train end users and provide support to the release of the solution *Hyland Note:* Training end users is a critical task for the OnBase team when new solutions are implemented. This task will require Cobb to define training procedures when releasing new capabilities to the business

---

[1] The actual number of days for each task will vary by project. Cobb IS and Harvest will estimate the duration/effort during project planning steps.
[2] It will be very important for Cobb/Harvest to manage initial project scope. Best demonstrated practice is to give users time to use the solution for a period of time as non-essential requirements tend to change after use

Page **7** of **7**